物理乱数の発生とその性質(乱数プログラム・パッケージ)

AUTHOR(S):

宮武, 修; 一村, 稔

CITATION:

宮武, 修 ...[et al]. 物理乱数の発生とその性質(乱数プログラム・パッケージ). 数理解析研究所講究録 1983, 498: 89-98

ISSUE DATE:

1983-09

URL:

http://hdl.handle.net/2433/103636

数理解析研究所講究録
498巻 1983年 89-98

物理乱数の発生とその性質

阪電通大　宮武　修（Osamu Miyatake）
岡山理大　一村　稔（Minoru Ichimura）

本研究は著者が広大理学部の吉沢研究室と共同で行ったものである．以下主として0から9までの整数からなる一様乱数について述べるので，単に一様乱数または乱数といえば，ここでは上のような乱数列をさすものとする．MTに収蔵された吾々の乱数をMIKYとよぶことにする．

§1．物理乱数の必要性．

乱数には如何なる規則があってもいけない．ところで，数学とくに計算機で乱数を発生させようとすると，どうしてもある規則によるほかはないから，数学的手段で理想的な乱数を発生させることは不可能なこと思われる．

また乱数のユーザーの立場についていえば，実際に乱数の検定を一々おこなって計算をすすめる人はきわめて稀であろう．また乱数の検定に合格したからと言って，それが良い乱数であるとは必ずしも断定しがたい．

このような理由で，「検定を必要としない乱数列の発生は，吾々がもっとも望むところであって，そのためには乱数の発生機構そのものにさかのぼる必要がある．私たちはそれ故，

乱数の発生に物理現象を利用することにしたのである.

物理乱数の発生には, 理屈としては, 完全なサイコロを振ればよいのであるが, これは実行不可能であるので, これに代るものとして私たちは放射性核から放出されるガンマ線(γ線)を利用することにした. 原子核としては, 半減期が約28年である Cs^{137} (セシウム-137) を利用することにした. このように寿命が長い原子核の集りから出てくるγ線は互に独立に, しかもランダムに放射されることはほとんど疑問の余地がない.

物理乱数はこれまでほとんど利用されていない. その理由は次のようなものであると言われている[1]: (1)物理乱数には再生性がない, (2) 電子回路の作動に安定性がない, (3) 発生速度がのろくて電子計算機と歩調が合わない. これらの理由のうち, (1) と (3) とはMTや磁気ディスクの利用によって解決され, (2) については, 今日ではエレクトロニクスが十分発達していて, その心配はいらない. すなわち物理乱数を敬遠する理由は今日ではもはや存在しない.

§2 γ線による物理乱数の発生法.

γ線を物理乱数の発生源として用いる吾々の方法[2]にはつぎの利点がある: (1) γ線のエネルギーがバック・グラウンドの放射線のそれにくらべて格段に高いため, その識別が容易

である．(2) 確率計算が明快である．(3) 生成が速い．

吾々の装置の原理は図1に示されている．図のパルス発生器によって一定時間々隔でクロック・パルス (C.P.) が

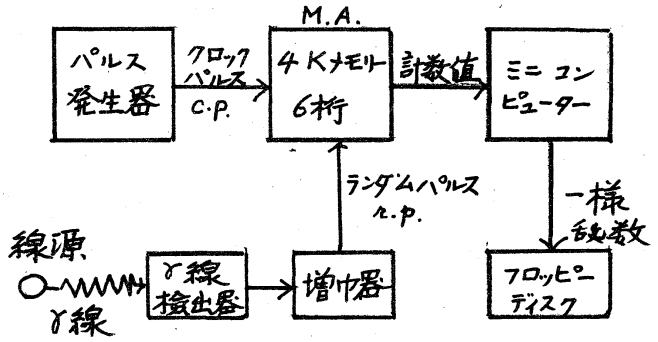

図1．乱数発生装置の原理図

Multichannel Analyser (M.A.) に送りこまれる．またγ線源によって発生されるランダム・パルス (R.P.) が M.A. に送りこまれる．M.A. には4096個のメモリーがあり，始め，これらはすべて clear されている．1つの R.P. によって第 i メモリーの gate がひらかれ，その次の R.P. によって gate は閉ざられ同時に第 $i+1$ メモリーの gate がひらかれる．そしてこの間にやってくる C.P. の個数が第 i メモリーに記銘される．この個数を n_i とする．これらの事情は図2に示されている．

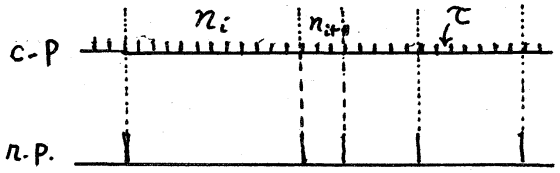

図2 クロック・パルスの計定

このようにして4096個のメモリーにおける C.P. のカウントがえられる．これらを順に

$$n_1,\ n_2,\ \cdots,\ n_{4096}$$

とする．次にこれらの n_i をそのままにしておいて，再び第1から第4096のメモリーにおいて C.P. のカウントを行い，

これらを順に

$$n_1', \ n_2', \ \cdots, \ n_{4096}'$$

とする．更にもう一巡してカウント

$$n_1'', \ n_2'', \ \cdots, \ n_{4096}''$$

がえられる．このようにしてオイメモリーにおいては和 $n_i + n_i' + n_i''$ がえられ，これから

$$n_i + n_i' + n_i'' \equiv I_i \pmod{10}, \quad (0 \leqq I_i \leqq 9)$$

によって４０９６個の整数列

$$I_1, \ I_2, \ \cdots, \ I_{4096}$$

がえられる．これらを順にフロッピー・ディスクに記録する．以上の操作が終ってから，すべてのメモリーを clear する．そして以上の操作を何度もくり返して整数列 $\{I_n\}$ をつくると，これが吾々が求める一様整数乱数列である．

吾々の方法では，C.P. の勘定を３巡させ，１つの乱数 I_i をつくるために３つの n_i, n_i', n_i'' を用いた．この巡回数は多いほど乱数の精度が上る．また γ線の平均計数 N/sec と C.P. の時間々隔で sec との積 $\lambda = N$ では乱数の精度を決定し，３巡回の場合には精度 $\propto \lambda^3$ である[2]．吾々の場合には $\lambda = 4 \times 10^{-3}$ であって，整数Ｉの出現確率を P_I とし

$$P_I = \frac{1}{10}(1 + \varepsilon_I), \quad (0 \leqq I \leqq 9)$$

とおくと，$|\varepsilon_I| \leq 10^{-6}$ である．

§3．擬似乱数と検定

真の乱数列には，検定に引っかかる部分もなければならないから，いわゆる local randomness の条件を満足するものだけを採用するというやり方は果して妥当なものであるかどうかは大いに疑問である．しかし擬似乱数の周期性や格子構造[3]などは決定的に悪い性質であろう．次に格子構造に関することについて若干ふれることにする．

乗算合同法

$$I_n = k I_{n-1} + b \pmod{M}, \quad x_n = I_n / M \tag{1}$$

によってえられる乱数列 $\{x_n\}$ を考える．いま $n \geq 3$ とし，整数 $C_1, C_2, \cdots, C_n$ が2つの条件

$$\begin{aligned} &C_1 + C_2 k + \cdots + C_n k^{n-1} \equiv 0 \pmod{M}, \\ &b\left(C_2 + C_3(k+1) + \cdots + C_n(k^{n-2} + k^{n-3} + \cdots + k + 1)\right) \equiv 0 \pmod{M} \end{aligned} \tag{2}$$

を満足するときは，(1)からつくった相つぐ乱数の組

$$(x_1, x_2, \cdots, x_n) \tag{3}$$

は超平面

$$C_1 x_1 + C_2 x_2 + \cdots + C_n x_n = 0, \pm 1, \pm 2, \cdots$$

のいづれかの上にのっている．これは Marsaglia の証明[3]

を真似て証明することができる．いま α_1，α_2，α_3 を任意の実数とし，3重積分

$$I=\int_0^1\int_0^1\int_0^1 \cos^2\{n\pi(\alpha_1 y_1+\alpha_2 y_2+\alpha_3 y_3)\}dy_1dy_2dy_3$$

$$=\frac{1}{2}\int_0^1\int_0^1\int_0^1\{1+\cos 2n\pi(\alpha_1 y_1+\alpha_2 y_2+\alpha_3 y_3)\}dy_1dy_2dy_3$$

は Riemann-Lebesque の定理によって $n\to\infty$ に対して $\frac{1}{2}$ に近づく．しかるにもし（3）のような擬似乱数を用いて，モンテカルロ法で I の値を求めることにすると

$$\cos^2\{n\pi(\alpha_1 x_1+\alpha_2 x_2+\alpha_3 x_3)\}=\cos^2\{n\pi((\alpha_1-C_1)x_1+(\alpha_2-C_2)x_2+(\alpha_3-C_3)x_3\}$$

（n は整数）

となるから，得られた I の値は真の値 $\frac{1}{2}$ と全く異るものになる．とくに $(\alpha_1,\alpha_2,\alpha_3)=(C_1,C_2,C_3)$ のときは誤った値 $I=1$ となり，Riemann-Lebesque の定理は成立しない．

乗算合同法（1）において $k=65539$，$b=0$，$M=2^{32}-1$ とおいたものは，あまりよくない乱数を発生することは今日ではよく知られているが，一時は盛んに用いられたものである．いまこの乱数を用いて直径が1である3次元球の体積を求めた結果を図3に示す．図の黒丸がそれで，白丸は各々のMIKY乱数による結果である．真の値は $V=0.5236$ で…

図の破線は68%の信頼限界を示す.

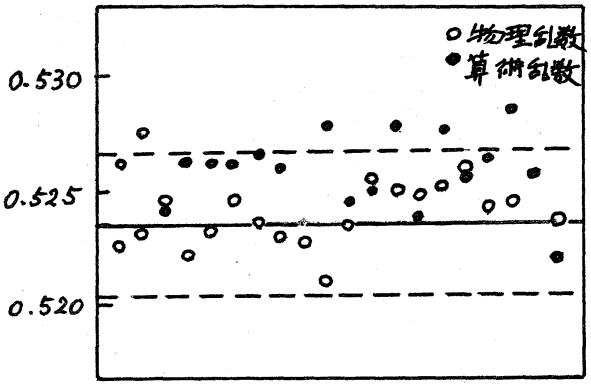

図3 球の体積(直径1)のモンテ・カルロ計算. 破線は68%の信頼限界を示す.

M系列においても色々な困難がおこる. たとえば, 原始多項式 D^p+D^q+1 を用いて生成したM系列[4]では, 生成された乱数列の遷移行列をつくってみると, それは独立な数列による遷移行列から著しくかたよることが示される.

§4. 物理乱数の使用法.

注意してつくられた物理乱数は完全なサイコロを振ることと等価であるから, 理想的なものと言ってよい. しかし算術乱数の場合のように, 簡単に subroutine subprogram を数行書き下せばよいというように手軽にはいかない. それ故普通の擬似乱数で十分間にあう場合には敢て物理乱数を使う必要はないであろう. 物理乱数がその効力を発揮するのは次のような場合であろう:

(i) 多次元の問題,

(ii) standard として使用される分布曲線をつくる場合,

(iii) 非常にデリケートなシミュレーションにおいて, ある稀現象が起るかどうかをしらべる場合.

上記(i)について言えば，例えば，粒子の散乱問題と考えると，1つの事象を起させるのに，多くの乱数の組が必要になる．このような場合には擬似乱数はほとんど無力である．

(ii)について言えば，例えば中心極限定理によると，

$$\overline{X}=\frac{1}{n}(X_1+X_2+\cdots+X_n)$$

はれが大きければ正規分布に近い分布を示すがれが小さいときの分布はどうか，と言った問題である．図4は分布密度

$$S(x)=\frac{1}{\pi\sqrt{1-x^2}}$$

を用いてつくった平均値 $\overline{x}$ の分布密度を物理乱数MIKYを用いてつくって示したものである．このような曲線を解析的に求めることは不可能に近く，また擬似乱数によっては信用できる曲線がえられない．

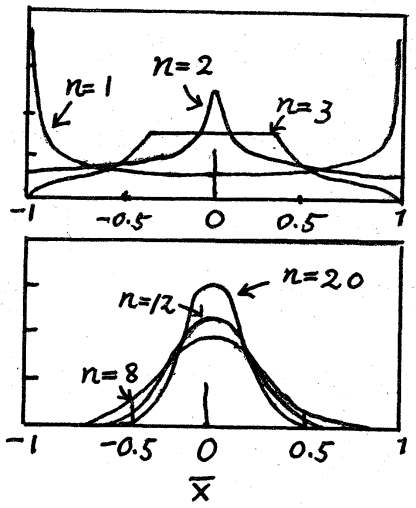

図4. $S(x)=\frac{1}{\pi\sqrt{1-x^2}}$ を用いた $\overline{x}=\frac{1}{n}\sum x_i$ の分布

上記(iii)については，真の乱数，したがって物理乱数を必要とすることは明かであろう．

§5. 結論

吾々は物理乱数MIKYに対して種々の検定を試みた．そ

して結果はすべて満足すべきものであった．確率論が示す割合で，検定不合格の場合もあらわれた．しかし不合格だからといって，吾々は不合格になった部分をすてると言うようなことはしない．

吾々の方法はγ線の1つ1つの出現を問題にするのであるから，その確率論的処理は明快である．γ線の代りにα線を用いてもよい．

現在，吾々の乱数MIKYは2億個の整数をふくみ，4個のMTに収められている．そしてこれらは需要者に実費で配布することにしている．

尚，正規乱数も目下物理的に作成する予定である．すでに得られた一様乱数をBox-Müllerの法で変換する方法も考えられるが，この方法には誤差が起ることが考えられる．γ線では，χ^2_{2n}-乱数はもっとも簡単に生成できる．そこでこのような乱数を2つとり，それらをχ'^2_{2n}，χ''^2_{2n}としたとき差$\Delta = \chi'^2_{2n} - \chi''^2_{2n}$が正規分布になる（大きなnについて）ことを利用して正規乱数をつくるのである．

参考文献

(1) B. Jansson, Random Number Generators (Victor Pettersons Bokindustri Aktiebolag, Stockholm, 1966).

(2) O. Miyatake, H. Inoue and Y. Yoshizawa, Generation of Physical Random Numbers, Math. Janonica 20 (1975) 207; O. Miyatake, Y. Yoshizawa, H. Inoue, H. Kumahora, M. Ichimura and H. Kimura, On the Generation and Properties of Physical Random Numbers, Math. Japonica 24 (1979) 369; 吉沢, 井上, 宮武, 物理乱数の特徴と算術乱数の欠点, 日本物理学会誌, 36 no.12 (1981), 885; H. Inoue, H. Kimura, Y. Yoshizawa, M. Ichimura and O. Miyatake, Random Numbers Generated by a Physical Device, Appl. Statist (London) 32 no. 2 (1983).

(3) G. Marsaglia, Random Numbers fall mainly in the Planes, Proc. Nat. Acad. Sci., 61 (1968) 25

(4) 手塚集, 伏見正則, 最大同期列を用いた, ある種の一様乱数発生法とその改善, 応用統計学研究会 (1980).